


Security Aspects of Biometric System Evaluation

February 14th, 2002

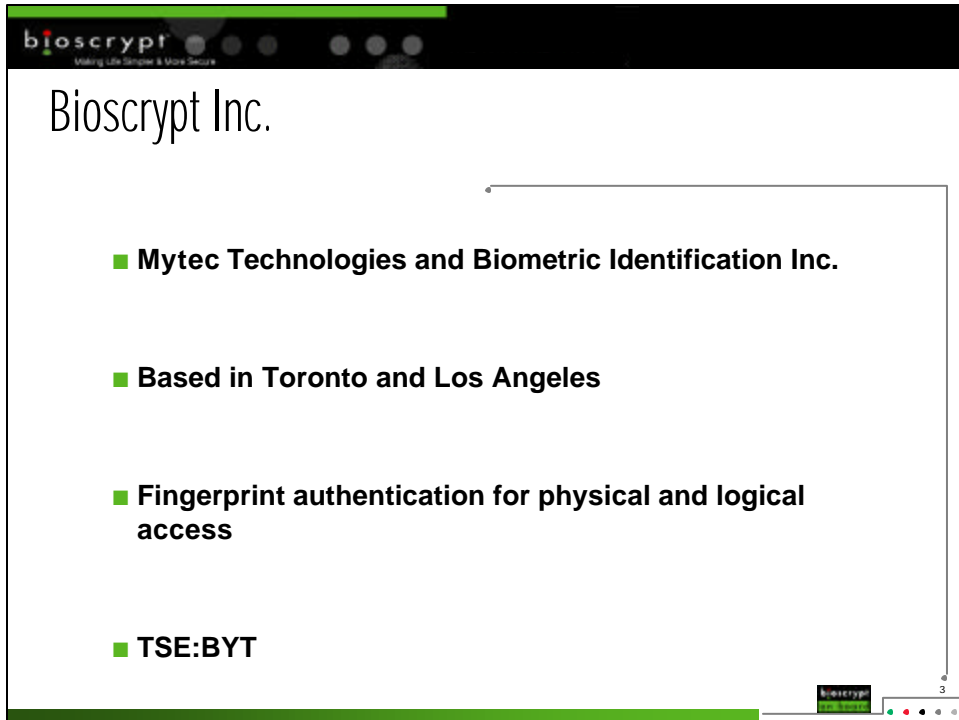
Colin Soutar, CTO
Bioscrypt Inc.

"...there is more to a security system than just a biometric device..."



Presentation Outline

- Company Overview
 - Bioscrypt Inc.
- Bioscrypt Technology
- Evaluated Product
 - Bioscrypt Enterprise for NT Logon
- Vulnerabilities Addressed
 - Cryptography and Biometrics
- Conclusions

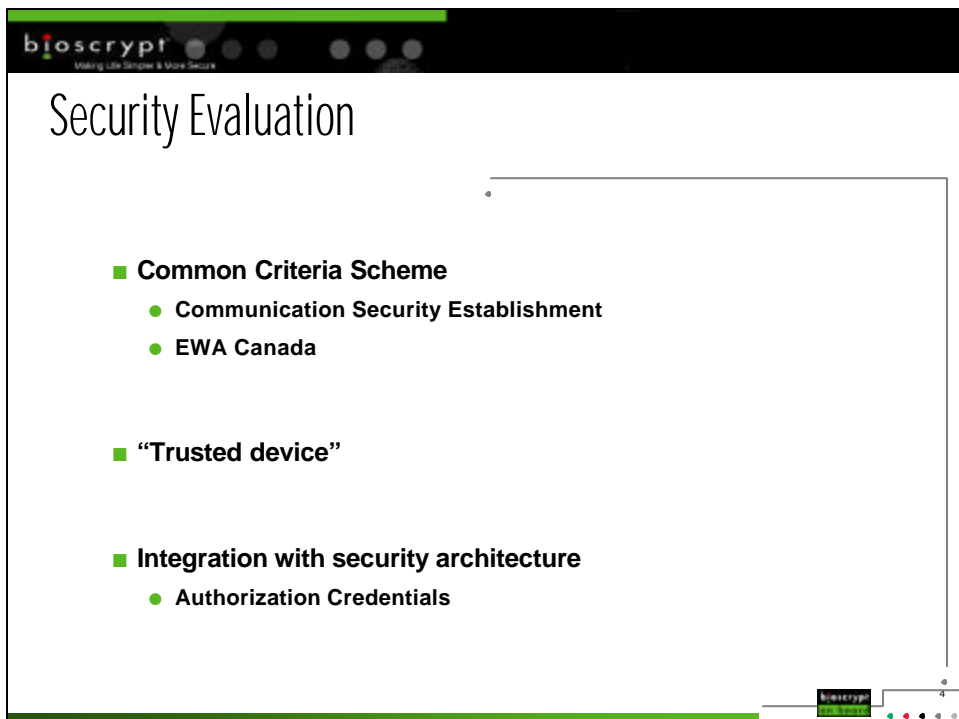
A presentation slide for Bioscrypt Inc. The slide has a black header with the 'bioscrypt' logo and the tagline 'Making Life Simpler & More Secure'. The main content area is white with a green border. It lists four bullet points: 'Mytec Technologies and Biometric Identification Inc.', 'Based in Toronto and Los Angeles', 'Fingerprint authentication for physical and logical access', and 'TSE:BYT'. The slide number '3' is in the bottom right corner.

bioscrypt
Making Life Simpler & More Secure

Bioscrypt Inc.

- **Mytec Technologies and Biometric Identification Inc.**
- **Based in Toronto and Los Angeles**
- **Fingerprint authentication for physical and logical access**
- **TSE:BYT**

3

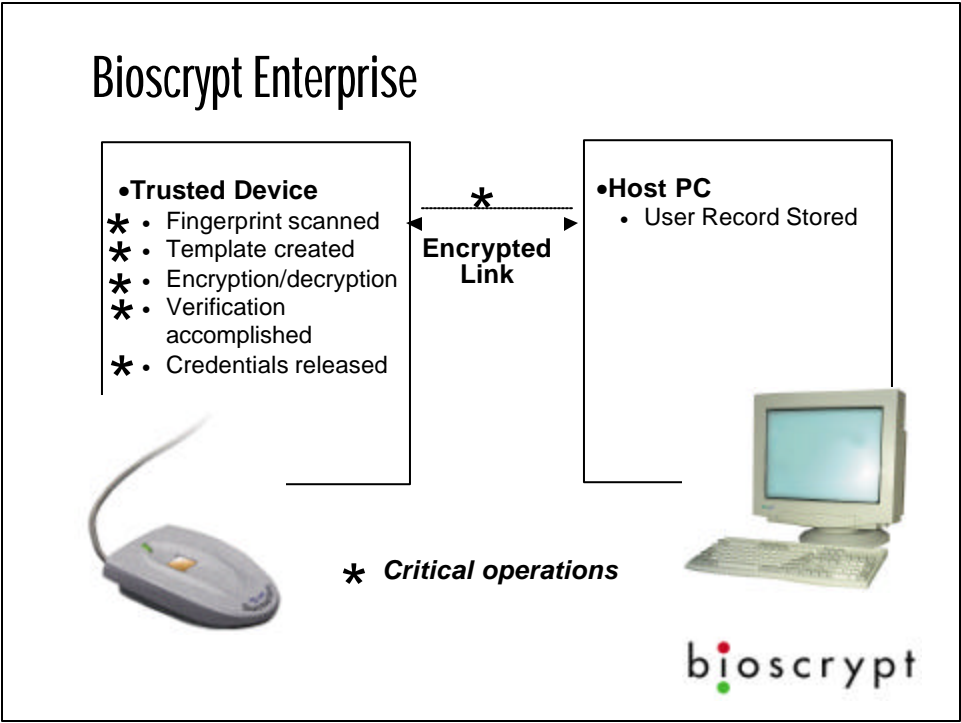
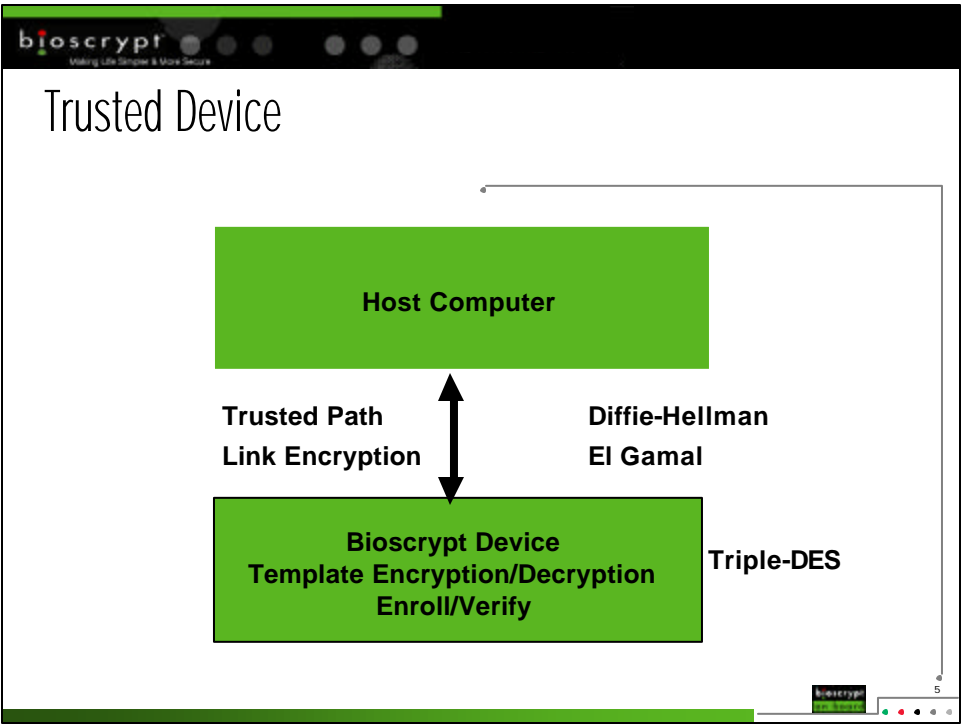
A presentation slide for Bioscrypt Inc. The slide has a black header with the 'bioscrypt' logo and the tagline 'Making Life Simpler & More Secure'. The main content area is white with a green border. It lists three bullet points: 'Common Criteria Scheme' (with sub-bullets 'Communication Security Establishment' and 'EWA Canada'), '“Trusted device”', and 'Integration with security architecture' (with sub-bullet 'Authorization Credentials'). The slide number '4' is in the bottom right corner.

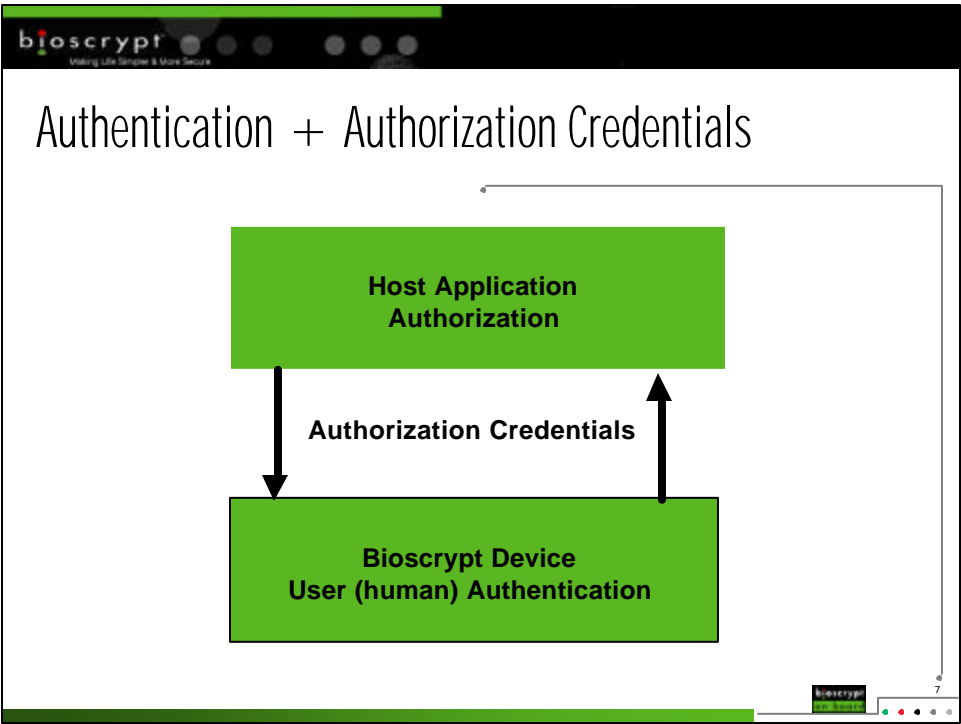
bioscrypt
Making Life Simpler & More Secure

Security Evaluation

- **Common Criteria Scheme**
 - Communication Security Establishment
 - EWA Canada
- **“Trusted device”**
- **Integration with security architecture**
 - Authorization Credentials

4





Authorization Credentials

- Examples of Credentials
 - password, PIN, private key → signed data

Benefits

- Link between User Authentication and Authorization
- Complex authentication “answer”
 - API’s (BioAPI, CDSA/HRS)
- Single user - multiple system identities (Roles)

The slide features a dark header with the 'bioscrypt' logo and the tagline 'Making Life Simpler & More Secure'. The main title is 'Data structure – User Record'. A diagram on the left shows a dashed box containing two green rectangles: the top one is labeled 'Authorization Credentials' and the bottom one is labeled 'Biometric Template'. To the right of the diagram, the text '3-DES Encrypted Device Key' and 'FIPS 46-3 and FIPS 81' is displayed. At the bottom, a statement reads 'User record can be stored in clear – prevents “Identity Theft”'. The bottom right corner includes a small 'bioscrypt' logo and a page number '9'.

bioscrypt
Making Life Simpler & More Secure

Data structure – User Record

Authorization
Credentials

Biometric Template

3-DES Encrypted Device Key
FIPS 46-3 and FIPS 81

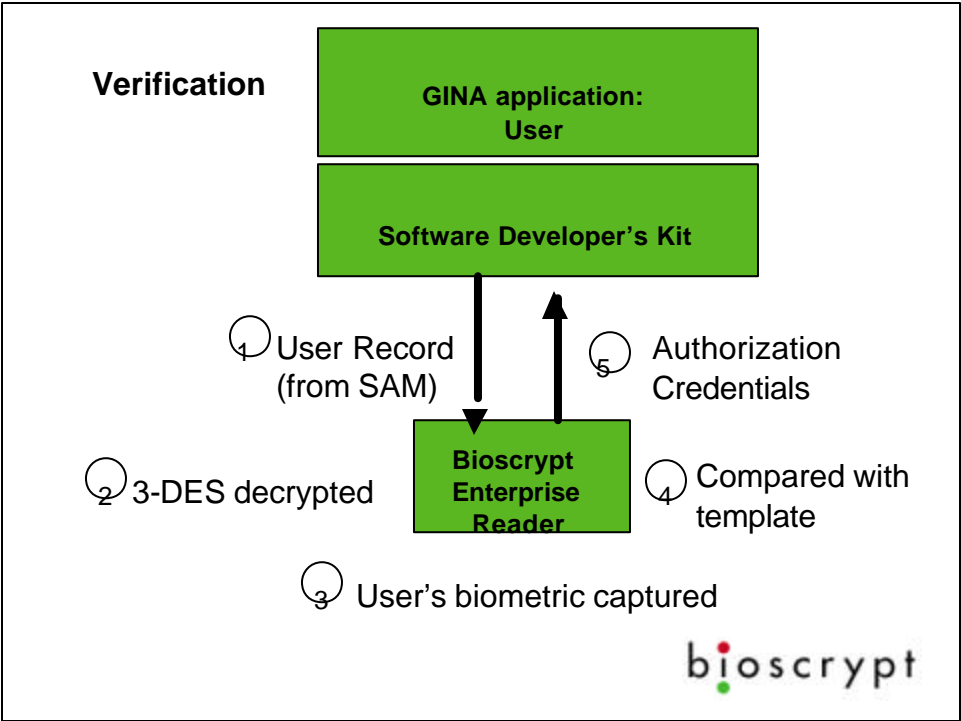
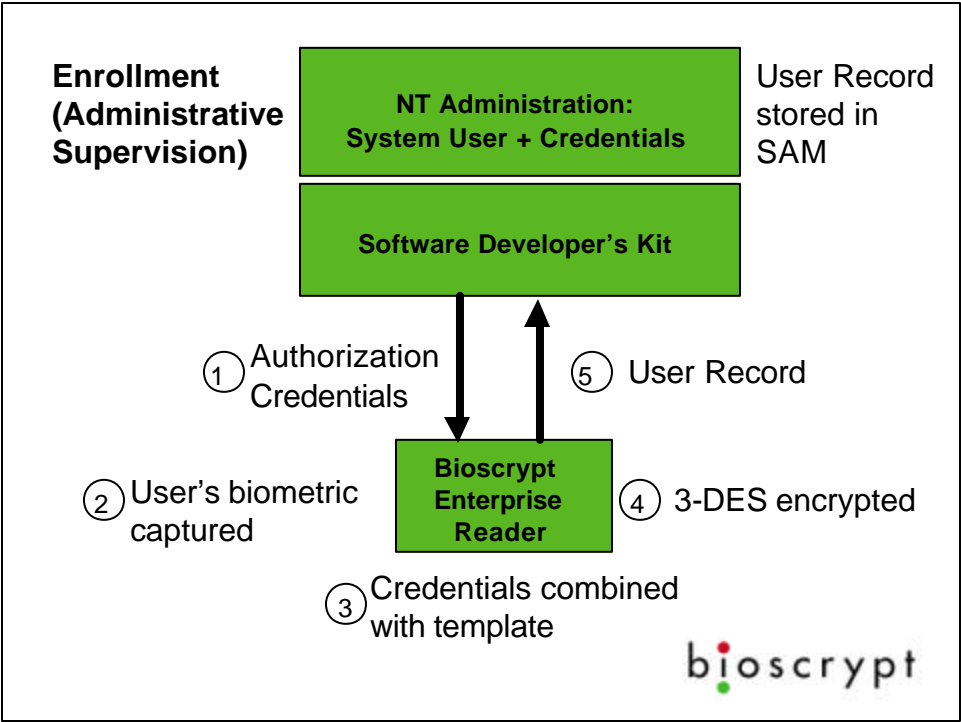
User record can be stored in clear – prevents “Identity Theft”

bioscrypt
Making Life Simpler & More Secure

9

Evaluated Product

- **Authorization Credentials**
 - User Password
- **Application**
 - Replacement for the Microsoft GINA



bioscrypt

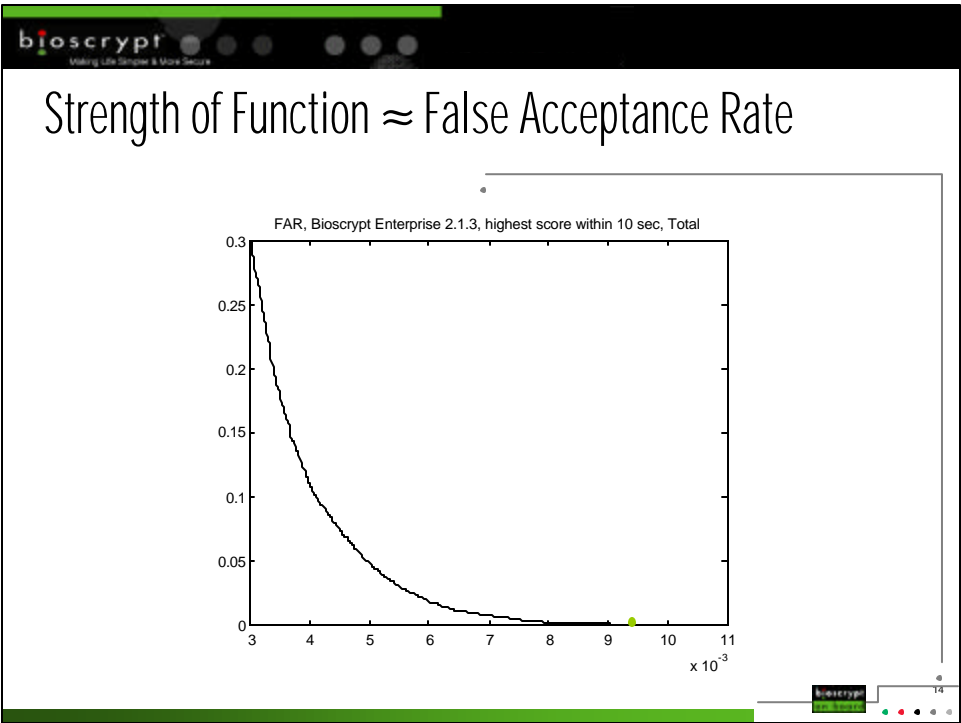
Making Life Simpler & More Secure


Vulnerabilities

- Confidentiality of biometric data/user credentials
 - 3-DES Encryption
- Data Integrity
 - Link encryption
- Replay Attack
 - Authorization Credentials, Unique session key
- Biometric Performance
 - Strength of Function

bioscrypt



13





Statistical Confidence – Cost of Testing

- Number of trials limits the extent of the performance claim
- Tests are expensive
- $n = 14,111 \rightarrow \text{FAR} \approx 0.001$
- Based on normal approximation
 $\sigma \approx 0.0245$, and so $\varepsilon = z \cdot \sigma / \sqrt{n} \approx 0.00034$.
Thus, we have 95% confidence that $\text{FAR} = 0.0006 \pm 0.0003$, or $1/1000$.



Conclusions

- Biometrics can be evaluated within a security context
- Powerful combination with cryptography
- Common Criteria Evaluation for biometrics
 - Methodology evaluation working group
 - Biometric Protection Profiles

colin.soutar@bioscrypt.com

